Exhibit R to the Declaration of Imran A. Khaliq In Support Of Visto's Opening Claim Construction Brief Under P.R. 4-5(a)

PATENT

SYSTEM AND METHOD FOR ENABLING SECURE ACCESS TO SERVICES IN A COMPUTER NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to co-pending patent application entitled "System and Method for Globally Accessing Computer Services," serial number 08/766,307, filed on December 13, 1996, by inventors Mark D. Riggins, R. Stanley Bailes, Hong Q. Bui, David J. Cowan, Daniel J. Mendez, Mason Ng, Sean Michael Quinlan, Prasad Wagle, Christine C. Ying, Christopher R. Zuleeg and Joanna A. Aptekar-Strober, which subject matter is hereby incorporated by reference. This related application has been commonly assigned to RoamPage, Inc.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly to a system and method for enabling secure access to services in a computer network.

2. Description of the Background Art

In its infancy, the Internet provided a research-oriented environment where users and hosts were interested in a free and open exchange of information, and where users and hosts mutually trusted one another. However, the Internet has grown dramatically, currently interconnecting about 100,000 computer networks and several million users. Because of its size and openness, the Internet has become a target of data theft, data alteration and other mischief.

Virtually everyone on the Internet is vulnerable. Before connecting, companies balance the rewards of an Internet connection against risks of a security breach. Current security techniques help provide client and server authentication, data confidentiality, system integrity and system access control.

The most popular of the current security techniques is a firewall, which includes an intermediate system positioned between a trusted network and the Internet. The firewall represents an outer perimeter of security for preventing unauthorized communication between the trusted network and the Internet. A firewall may include screening routers, proxy servers and application-layer gateways.

For users on the internet to gain access to protected services on the trusted network, they may be required to provide their identity

to the firewall by some means such as entering a password or by computing a response to a challenge using a hardware token. With proper authentication, the user is allowed to pass through the firewall into the local network, but is typically limited to a predetermined set of services such as e-mail, FTP, etc.

Some local network managers place just outside the firewall a server, often referred to as a "sacrificial lamb" for storing non-confidential data which is easily accessible by the remote user but providing little security.

A De-Militarized Zone, or DMZ, sits between two firewalls protecting a trusted network. The external firewall protects servers in the DMZ from external threats while allowing HyperText Transfer Protocol (HTTP) requests. The internal firewall protects the trusted network in the event that one of the servers in the DMZ is compromised. Many companies use DMZs to maintain their web servers.

Another security technique for protecting computer networks is the issuance and use of a public key certificates. Public key certificates are issued to a party by a certificate authority, which via some method validates the party's identity and issues a certificate stating the party's name and public key. As evidence of authenticity,

the certificate authority digitally signs the party's certificate using the certificate authority's private key.

Thus, when a user via a client computer connects to a server, the client computer and server exchange public key certificates. Each party verifies the authenticity of the received certificates by using the certificate authority's public key to verify the signature of the certificate. Then, by encrypting messages with the server's public key the user can send secure communications to the server, and by encrypting messages with the user's public key the server can send secure communications to the user. Although any party might present a public key certificate, only the real user and the real host have the corresponding private key needed to decrypt the message. Examples of authentication and key distribution computer security systems include the Kerberos™ security system developed by the Massachusetts Institute of Technology and the NetSP™ security system developed by the IBM Corporation.

These security techniques do not, however, solve problems associated with ~~the~~ a roaming (traveling) user. For the roaming user, maintaining identification and authentication information such as passwords, certificates, keys, etc. is a cumbersome process. Further, accessing multiple systems requires multiple keys, which often are too complex to track and use. Also, direct access to systems behind

firewalls compromises security. Therefore, a system and method are needed to enable remote access to computer services easily and securely.

SUMMARY OF THE INVENTION

The present invention provides a system and method for enabling secure access to services in a computer network. The network system includes a global server coupled via a computer network to computer services. The global server includes a communications engine for establishing a communications link with a client; security means coupled to the communications engine for determining client privileges; a servlet host engine coupled to the security means for providing to the client, based on the client privileges, an applet which enables I/O with a secured service; and a keysafe for storing keys which enable access to the secured services. The global server may be coupled to multiple sites, wherein each site provides multiple services. Each site may be protected by a firewall. Accordingly, the global server stores the keys for enabling communication via the firewalls with the services.

A method includes the steps of establishing a communications link with a client; identifying and authenticating the client; determining client privileges; providing to the client, based on